

Home Wi-Fi safety checklist

CyberGuardLab is an independent comparison site. We may earn a commission on paid links; buying nothing is valid.

Lock the router you already own before you shop for a Wi-Fi inspector. An inspector is a flashlight. It is not the lock.

1. Change the router admin password so it is not the Wi-Fi passphrase. Update firmware.
2. Prefer WPA3, or WPA2-AES if an old TV blocks you. Disable WPS and remote administration from the WAN.
3. Put cameras and cheap IoT on a guest network. Keep laptops and phones on the main SSID.
4. Look at the DHCP client list. Name the devices you recognize. Kick the ones you do not.
5. If you still install an inspector, run it once and write down every finding you actually fixed.
6. On public Wi-Fi, use a VPN for the session you care about. Do not send bank passwords on a captive portal you do not trust.
7. Keep an offline backup. A ransomware shield is a seatbelt; a backup is the spare car.

A full-screen 'call this number' page is a tech-support scam, not a router finding. Close it in Task Manager. FTC: consumer.ftc.gov.

Webcam software cannot beat a closed shutter. Cover the laptop camera if you want a physical guarantee.

CyberGuardLab.com key points | August 21, 2026